Remarks/Arguments:

The present invention relates to a network system wherein a home server is protected by a firewall. Specifically, a network security managing section architects a network security system **in response to a user connection request**.

On page 3, the Official Action objects to claims 2, 3, 6-8, 10, 17, 18, 21-23 and 25 because they recite "the plurality of web terminals", "the network security system" or "the web terminal". Claims 2, 3, 6, 7, 10, 17, 18, 20, 21 and 25 have been amended to show antecedent basis as requested by the Official Action. Claims 8 and 23, however, do not need to be amended because they recite "the network security system" in which antecedent basis is supported in the preamble. Withdrawal of the claim objection is respectfully requested.

On page 3, the Official Action rejects claims 1-2, 4-6, 16-17 and 19-21 under 35 U.S.C.103(a) as being unpatentable over Sharood (US 6,453,687) in view of Syvanne US Publication No. 2003/0097590). Furthermore, page 2 of the advisory action disagrees with the Applicants' request for reconsideration. It is respectfully submitted, however, that the claims are patentable over the art of record for the reasons set forth below.

Sharood teaches a system for monitoring appliances such as a dishwasher, gas range and water heater. Specifically, these appliances are monitored over the internet. Syvanne teaches a personal firewall for protecting a computer. Specifically, the personal firewall detects its location and automatically uses predefined security rules for that specific network.

Applicants' invention as recited by currently amended claim 1, includes a feature which is neither disclosed nor suggested by the art of record, namely:

> ...**said provider controls said network security managing section to initiate installation and setting changes of such firewall responsive to a connection request from said home server.**

Claim 1 relates to a network security managing section of a provider. When a home server requests a connection to the internet, the provider controls the network security managing section to install a firewall in order to protect the home server. This feature is found in the originally filed application in Fig. 1 and furthermore on page 5, lines 13-25. No new matter has been added.

In paragraph [0010], Syvanne teaches a personal firewall for a computer device wherein different sets of predefined rules are used in different networks (*"personal firewall is provided with different sets of security rules"*). Furthermore, paragraph [0010] teaches that the personal firewall detects its current network location and activates a given set of predefined security rules in response to the detected location (*"the personal firewall activates one of a given sets of security rules according to the detected current location of the computer device...the personal firewall automatically uses the security rules predefined for the network to which the computer device is connected"*). Syvanne's firewall, **selects predefined settings based on its current location**. For example, if the firewall detects that the computer device is in a home network, minimal restrictions may be selected (user should not be restricted in his home network). In another example, if the firewall detects the computer device is in a company network, firewall settings with restrictions defined by that particular network will be selected (company may want to restrict access). Syvanne's firewall allows a computer device to adapt its firewall settings to any particular network that it may be connected to. Furthermore, paragraph [0013] of Syvanne teaches that the predefined security rules are updated by a centralized rule-based server (*"updated and distributed centrally by a centralized rule-based server"*). Specifically, in order to keep updated rules, the personal firewall queries the centralized management server for updates of security rules (*"personal firewall is configured to periodically query the availability of the updated security rules from the centralized management"*). Syvanne's system is shown in Fig. 1, where a personal firewall resides on laptop 1 and personal firewall management 8 is utilized to update the security rules for the firewall.

Applicants' claim 1 is different than Syvanne, because the addition of the **provider controlling the managing section to install and modify the firewall responsive to the home server connection request** (*"provider controls said* *network security managing section to initiate insulation and setting changes of said firewall responsive to a connection request from said home server"*). The process described in Applicants' claim 1 can be described in reference to Fig. 1. Home server 15 sends a connection request to the internet connecting section 12 of provider 11. In response to this connection request the internet connecting section 12 controls the network security managing section 13 of provider 11. Network security managing section 13 then initiates the installation and setting changes of a firewall on the users network security system 17. At this point, network security system 17 utilizes a newly installed firewall to protect home server 15 during connection to internet 10. This process, as shown in Applicants' Fig. 1 below, ensures that the home server is protected from, for example, viruses and unwanted intruders before connecting to internet 10. In contrast, Syvanne's system, teaches selecting predetermined firewall settings based on network location. Syvanne does not suggest the provider installing and initiating firewall settings responsive to a connection request from a home server.

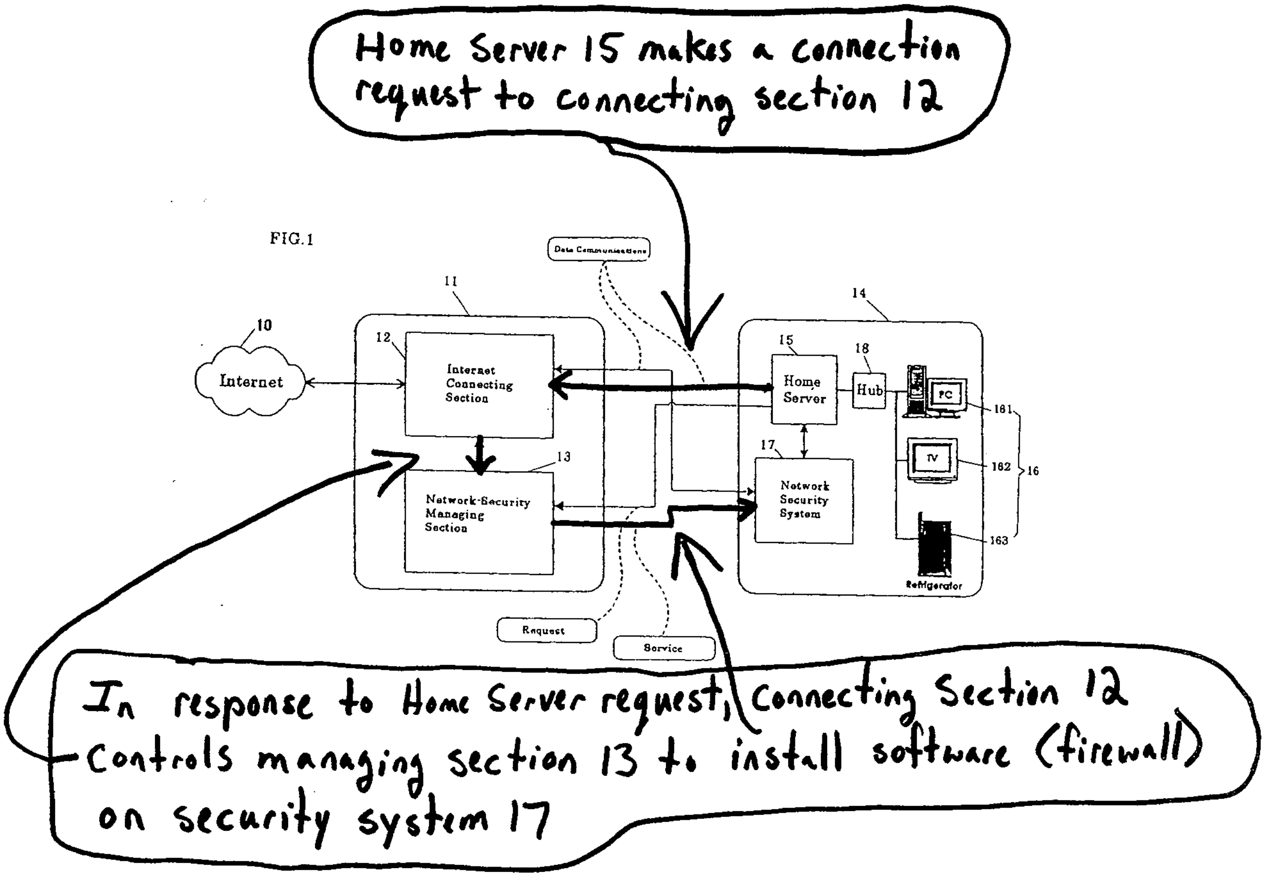
FIG.1

Home Server 15 makes a connection request to connecting section 12

In response to Home Server request, Connecting Section 12 Controls managing section 13 to install software (firewall) on security system 17

It is because Applicants include the feature of "*provider controls said network security managing section to initiate installation and setting changes of said firewall responsive to a connection request from said home server*", that the following advantages are achieved. An advantage is the ability for the home server to connect to the internet without the responsibility of architecting a network security system (**the provider is responsible for architecting the network security system that protects the home server**). Accordingly, for the reasons set forth above, claim 1 is patentable over the art of record.

Independent claim 16 includes all the features of claim 1. Thus, claim 16 is also patentable over the art of record for the reasons set forth above.

Dependent claims 2-15 include all the features of claim from which they depend. Thus, claims 2-15 are also patentable over the art of record for the reasons set forth above.

Dependent claims 7-30 include all the features of claim 16 from which they depend. Thus claims 7-30 are also patentable over the art of record for the reasons set forth above.

In view of the amendments and arguments set forth above, the above identified application is in the condition for allowance which action is respectfully requested.

Respectfully submitted,

RatnerPrestia

Lawrence E. Ashery, Reg. No. 34,515
Attorney for Applicants

LEA/RAE/dmw
Dated: January 18, 2008

P.O. Box 980
Valley Forge, PA 19482-0980
(610) 407-0700

NM238811